



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re the Application of

Takanori MASUI et al.

Application No.: 10/653,219

Filed: September 3, 2003

Docket No.: 116972

For: APPARATUS AND METHOD FOR SECURELY REALIZING COOPERATIVE
PROCESSING

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-082323 filed March 25, 2003

In support of this claim, a certified copy of said original foreign application:

☒ is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/tmw

Date: November 12, 2003

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 2 5 日
Date of Application:

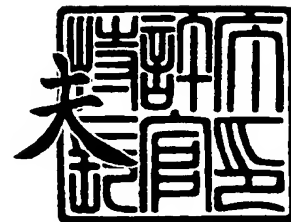
出 願 番 号 特 願 2 0 0 3 - 0 8 2 3 2 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 8 2 3 2 3]

出 願 人 富 士 ゼ ロ ッ ク ス 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 1 0 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 0 8 1 8 5 1

【書類名】 特許願

【整理番号】 FE03-00391

【提出日】 平成15年 3月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

 【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

 【氏名】 益井 隆徳

【発明者】

 【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

 【氏名】 横濱 竜彦

【発明者】

 【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株式会社内

 【氏名】 佐竹 雅紀

【特許出願人】

 【識別番号】 000005496

 【氏名又は名称】 富士ゼロックス株式会社

【代理人】

 【識別番号】 100075258

 【弁理士】

 【氏名又は名称】 吉田 研二

 【電話番号】 0422-21-2340

【選任した代理人】**【識別番号】** 100096976**【弁理士】****【氏名又は名称】** 石田 純**【電話番号】** 0422-21-2340**【手数料の表示】****【予納台帳番号】** 001753**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 情報処理装置及び方法

【特許請求の範囲】

【請求項 1】 指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施す署名部と、

前記署名部により電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部と、
を備えることを特徴とする情報処理装置。

【請求項 2】 請求項 1 に記載の情報処理装置であって、

前記署名部は、サービスを依頼した依頼者の電子署名を施すことを特徴とする情報処理装置。

【請求項 3】 請求項 1 に記載の情報処理装置であって、

前記署名部は、自装置の電子署名を施すことを特徴とする情報処理装置。

【請求項 4】 請求項 3 に記載の情報処理装置であって、

自装置は、サービスを発行する発行元装置であることを特徴とする情報処理装置。

【請求項 5】 請求項 3 に記載の情報処理装置であって、

自装置は、一のジョブ処理装置と他のジョブ処理装置との間を中継してジョブ処理された結果を転送する中継装置であることを特徴とする情報処理装置。

【請求項 6】 請求項 1 に記載の情報処理装置であって、

前記署名部は、電子署名付与の対象とする処理記述より後に処理を実行すべき処理記述を含めて署名することを特徴とする情報処理装置。

【請求項 7】 請求項 1 に記載の情報処理装置において、

前記署名部は、各ジョブ処理装置の実行対象となる複数の部分について、それぞれ電子署名を施すことを特徴とする情報処理装置。

【請求項 8】 請求項 1 に記載の情報処理装置において、

前記署名部は、処理記述の処理単位に電子署名を施すことを特徴とする情報処理装置。

【請求項 9】 指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現するためにコンピュータが実行する情報処理方法であって、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施し、

電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信することを特徴とする情報処理方法。

【請求項 1 0】 指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現させるコンピュータのプログラムであって、

コンピュータに、

前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施す手順と、

電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する手順と
を実行させるためのプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ネットワーク上に存在する様々な処理装置を連携させることで、多様な連携処理を実現するための技術に関し、特に連携処理におけるセキュリティ技術に関する。

【0 0 0 2】

【従来の技術】

スキャナ、ファクシミリ装置、プリンタ、複写機、及びそれらの機能を統合した複合機を LAN（ローカルエリアネットワーク）に接続し、パーソナルコンピ

ュータやメールサーバなどの情報処理装置と連携させ、オフィス作業用の各種サービスを提供するワークフローシステムが提案されている。

【0 0 0 3】

また近年、インターネット上に散在する各種ウェブアプリケーションを連携させる技術が提案されている。インターネット上にある多様な提供者が提供するアプリケーションサービスを連結して1つのシステムを構成できると、様々な既存サービスを利用することができるのでシステム開発コストが大幅に低減できると期待されている。また、このような連携的なサービスを実現するための共通の基盤としてXML (eXtensible Markup Language)等の言語が注目されている。

【0 0 0 4】

また、従来のワークフローシステムとしては、特許文献1や特許文献2、特許文献3に示されるものが知られている。また、ワークフロートは無関係であるが、電子署名に関する従来技術として特許文献4に示すものがある。この文献には、プログラムコードをセキュアに実行するコンピュータシステムにおいて、暗号化したプログラムコードに対しメモリ割当の最小単位ごとに電子署名を付すことで、署名検証や復号の処理をマルチタスク実行可能とする点が示されている。

【0 0 0 5】

【特許文献1】

特開平08-123744号公報

【特許文献2】

特開2002-099686号公報

【特許文献3】

特開2001-282970号公報

【特許文献4】

特開2002-353960号公報

【0 0 0 6】

【発明が解決しようとする課題】

フローを構成する各処理装置に対するサービスの要求は、何らかの指示データをその処理装置に送ることにより行われる。ここで、指示データの改ざんや、な

りすましなどの危険性があると、処理装置側が要求するセキュリティレベルを満足できない場合が出てくる。

【0 0 0 7】

現在のインターネット技術では、データの改ざん等の危険性を軽減する手段として、P K I（公開鍵基盤）における電子署名が用いられている。ところが、ワークフロー等の連携サービスでは、単なる電子署名技術だけでは以下のような理由から十分でない場合がある。

【0 0 0 8】

すなわち、処理装置にとっては、受け取った指示データが、連携サービスの要求者による指示内容の通りか否かが1つの重要な問題になる。ここで、ある処理装置が自分の受け取った指示データに対して加工を加えて次の処理装置に伝達するようなフローの仕組みも考えられるが、この仕組みでは、サービス要求者が最初に指示データに付した電子署名がフローの途中の処理装置で失われてしまうという問題がある。

【0 0 0 9】

【課題を解決するための手段】

本発明は、指示データに記述された処理記述に従って処理を実行する複数のジョブ処理装置を連携動作させることによりサービスを実現する情報処理装置であって、前記指示データに記述された処理記述に対し、各ジョブ処理装置の実行対象となる部分に電子署名を施す署名部と、前記署名部により電子署名が施された指示データを、前記処理記述の表わす処理を実行するジョブ処理装置に伝達すべく送信する送信部とを備える情報処理装置を提供する。

【0 0 1 0】

また本発明の好適な態様では、前記署名部は、サービスを依頼した依頼者の電子署名を施す。また別の好適な態様では、前記署名部は、当該情報処理装置の電子署名を施す。

【0 0 1 1】

また本発明のある態様では、前記情報処理装置は、前記サービスを発行する発行元装置である。例えば、発明の実施の形態の指示入力装置がこの発行元装置の

一例である。

【0012】

また別の態様では、前記情報処理装置は、一のジョブ処理装置と他のジョブ処理装置との間を中継してジョブ処理された結果を転送する中継装置である。例えば発明の実施の形態におけるフロー制御装置が、この中継装置の一例である。

【0013】

また本発明の好適な態様では、前記署名部は、電子署名付与の対象とする処理記述より後に処理を実行すべき処理記述を含めて署名する。

【0014】

【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。

【0015】

図1は、本発明に係るサービス提供システムのシステム構成パターンの一例を示す図である。このシステムは、指示入力装置10、フロー制御装置20、及び複数のアプリケーションサーバ25を含んでいる。

【0016】

アプリケーションサーバ25は、他の装置からの要求に応じて所定の処理サービスを提供するサーバである。例えば、サーバ25の例としては、例えば、文書データベースサーバや、メールサーバ、画像データに対して色変換や回転などの操作を施す画像処理サーバ等を挙げることができる。サーバ25は、そのような処理サービスを例えばウェブアプリケーションサービス等の形で提供する。

【0017】

このシステムは、あるサーバ25で文書を検索し、この結果検索された文書を別のサーバによって電子メールとして送信する、といった具合に、複数のサーバ25の処理を連携させた連携サービスを提供することができる。

【0018】

指示入力装置10は、このシステムに対するユーザの処理指示を入力するための装置である。ユーザは、指示入力装置10に対し、上述のような連携サービス

の実行指示を入力することができる。指示入力装置 1 0 は、例えばパーソナルコンピュータに、ユーザから本システムへの指示の入力を受け付けるためのユーザインタフェースプログラムを組み込んだものでよい。しかしながら、オフィスにおける文書処理サービスを想定すると、情報処理機能や通信機能に加え、紙文書を読み取って電子データ化する機能をも備えるデジタル複合機を指示入力装置 1 0 として用いることが好適である。デジタル複合機は、スキャナ、プリンタ、複写機、ファクシミリ、ネットワーク通信等の機能を併せ持つ。

【0 0 1 9】

フロー制御装置 2 0 は、各サーバ 2 5 に対して処理を依頼することで、それら個々のサーバ 2 5 が提供するサービスを連携した連携サービスを実現する。

【0 0 2 0】

好適には、指示入力装置 1 0、フロー制御装置 2 0 及び各サーバ 2 5 は、公開鍵暗号方式に対応しており、各自の秘密鍵、公開鍵を有している。また、指示入力装置 1 0、フロー制御装置 2 0 及び各サーバ 2 5 は、他の装置 1 0、2 0 やサーバ 2 5 の公開鍵を保持しているか、又は必要に応じてネットワーク上の認証局から取得することができる。

【0 0 2 1】

図 1 のシステムでは、ユーザが指示入力装置 1 0 に対して連携サービスの指示を入力すると、指示入力装置 1 0 がその指示内容を示したデータを送る。このデータを、以下ではフロー指示書 5 0 と呼ぶ。このフロー指示書 5 0 には、連携サービスに関与するすべてのサーバの処理内容の記述と、それら各処理の実行順序の情報が含まれている。フロー指示書 5 0 を受信したフロー制御装置 2 0 は、その指示書 5 0 に従って各サーバ 2 5 を制御することで、その指示書 5 0 が示す連携サービスを実現する。

【0 0 2 2】

このとき、フロー制御装置 2 0 は、受信したフロー指示書 5 0 に基づき各サーバ 2 5 への指示書（指示内容を示したデータ）5 2 を作成し、これら指示書 5 2 を各サーバ 2 5 に送ることで、それらサーバ 2 5 の連携動作を実現する。すなわち、フロー制御装置 2 0 は、フロー指示書 5 0 の記述に従い、次に動作させるべ

きサーバ 25 に対して指示書 52 を送信し、これに対してそのサーバ 25 から処理終了の通知（及び場合によっては処理結果のデータ）が返ってくると、その次のサーバ 25 に対して指示書 52 を送信する。

【0023】

このように図 1 のシステムは、サーバ 25 群がフロー制御装置 20 の制御の下に連携するという、いわばスター（星）型のシステム構成をとっている。

【0024】

次に、図 2 を参照して、本発明に係るサービス提供システムのシステム構成パターンの別の一例を説明する。図 2 において、図 1 に示したシステムの構成要素と同等の構成要素には同一符号を付して説明を簡略化する。

【0025】

このシステムは、指示入力装置 10 と複数のアプリケーションサーバ 25 とから構成されている。

【0026】

図 1 のシステムが連携制御のためのフロー制御装置 20 を有するのに対し、図 2 のシステムはそのような中央の制御装置を持たず、各アプリケーションサーバ 25 自身が連携動作のための制御動作を実行する。このため、指示入力装置 10 は、ユーザが指示した連携サービスのために各サーバ 25 が実行すべき処理を示したフロー指示書 50 を作成し、これを各サーバ 25 に送信して実行させる。

【0027】

図 2 の構成は、連携サービスを構成する各処理のための各サーバ 25 が、それぞれ各処理の順に並んだ、いわばデイジーチェーン（連鎖）型の構成となる。この構成では、サーバ連鎖の中の最初のサーバ 25-1 に対して指示入力装置 10 から指示書 50 を送信すると、これを契機にサービス処理が開始される。そして、サーバ 25-1 の処理が終了すると次のサーバ 25-2 の処理が開始され、このサーバ 25-2 の処理が終了するとその次のサーバ 25-3 の処理が開始されるといった具合に、各段階のサーバ 25 の間で処理が連携されていく。この場合、各サーバ 25 には、指示入力装置 10 から直接、又は前段のサーバ 25 から指示書 54 が送信される。そして、各サーバ 25 はその指示書に従って処理を実行す

るとともに、その指示書に示された次のサーバ25に対して処理開始の指示又は指示書54を送信する。このような仕組みで連携が実現される（詳細は後述）。

【0028】

以上、各サーバ25の連携の仕組みとして、フロー制御装置20により集中制御するフロー制御装置介在型と、各サーバ25が順に次のサーバ25に処理を受け渡すデ이지チェーン型の2つの仕組みを説明した。

【0029】

次に、連携サービスのために各サーバ25に送信される指示書52、54についての2つのタイプを説明する。

【0030】

第1は、連携サービスに関与する各サーバ25に対し、当該サーバ25への指示（該サーバ25の処理内容の記述）のみならず、他のサーバ25への指示をも含んだ指示書52又は54を送信する方式である。この方式の1つの例として、連携サービスに関与するすべてのサーバ25への指示を含んだ指示書を各サーバ25に送信する方式がある。このように、他のサーバ25への指示も含む形態の指示書を「包括指示書」と呼ぶこととする。

【0031】

第2は、連携サービスに関与する各サーバ25に対し、当該サーバ25への指示のみを含み、他のサーバ25への指示を含まない指示書52又は54を送信する方式である。このように、当該サーバ25への指示のみからなる指示書を「個別指示書」と呼ぶこととする。

【0032】

これら指示書52又は54の2つのタイプと、前述のシステム構成の2つのタイプを組み合わせれば、各サーバ25への指示書の送信形態としていくつかの送信形態が得られる。そのうちの代表的なものとして次の2つの指示送信形態を挙げることができる。

【0033】

まず第1は、図3に示すようなフロー制御装置介在型システムにおける指示送信形態である。

【 0 0 3 4 】

この指示送信形態では、まず指示入力装置 1 0 からフロー制御装置 2 0 に対し、サービスのために利用するすべてのサーバ 2 5 - 1, 2 5 - 2, 2 5 - 3 に対する個別指示書 6 2 - 1, 6 2 - 2, 6 2 - 3 を含んだ包括指示書 6 0 が送信される。1 つの例では、包括指示書 6 0 には、それら個別指示書 6 2 - 1, 6 2 - 2, 6 2 - 3 が、実行される順序に配列されている。フロー制御装置 2 0 は、受信した包括指示書 6 0 から各個別指示書 6 2 - 1, 6 2 - 2, 6 2 - 3 を取り出し、これらに対応するサーバ 2 5 - 1, 2 5 - 2, 2 5 - 3 にそれぞれ必要なタイミングで送信する。

【 0 0 3 5 】

第 2 の指示送信形態は、フロー制御装置非介在型システムに包括指示書を適用したものである。この形態の一例を図 4 に示す。

【 0 0 3 6 】

図 4 の形態では、まず指示入力装置 1 0 からフロー中の最初のサーバ 2 5 - 1 に対し、サービスのために利用するすべてのサーバ 2 5 - 1, 2 5 - 2, 2 5 - 3 に対する個別指示書 6 2 - 1, 6 2 - 2, 6 2 - 3 を含んだ包括指示書 6 0 が送信される。これを受け取ったサーバ 2 5 - 1 は、包括指示書 6 0 から自分宛の個別指示書 6 2 - 1 を識別し、これに従って処理を実行する。そしてサーバ 2 5 - 1 は、その包括指示書 6 0 から自分宛の個別指示書 6 2 - 1 を削除して新たな包括指示書 6 0 a を作成し、これをフロー中の次のサーバ 2 5 - 2 に送信する。次のサーバがどれかは包括指示書 6 0 内に記述されている。包括指示書 6 0 a を受信したサーバ 2 5 - 2 も同様に動作し、その包括指示書 6 0 a から自分宛の個別指示書 6 2 - 2 を削除して包括指示書 6 0 b を作成し、次のサーバ 2 5 - 3 に送る。このように第 2 の指示送信形態では、各サーバ 2 5 が包括指示書 6 0 から自分宛の個別指示書 6 2 を順次削除して次のサーバ 2 5 に受け渡していく。

【 0 0 3 7 】

上記第 1 及び第 2 の指示送信形態ではいずれも、指示入力装置 1 0 に対しユーザが連携サービスの実行を指示したとき、作成した包括指示書 6 0 のデータに対してそのユーザやその指示入力装置 1 0 の秘密鍵を用いて電子署名を施すことが

可能である。このため、その包括指示書 6 0 を直接受け取るフロー制御装置 2 0 やサーバ 2 5 - 1 なら署名検証によりその指示書 6 0 の改ざんの有無等を確認できる。このように、サービスを要求するユーザ自身の秘密鍵を用いて作成した電子署名や、その要求の入力に用いた指示入力装置 1 0 の秘密鍵を用いて作成した電子署名をイニシエータ (initiator) 署名と呼ぶことにし、そのユーザ及び指示入力装置 1 0 をイニシエータと総称することとする。イニシエータ署名として、ユーザの電子署名と指示入力装置 1 0 の電子署名のいずれを要求するかは、連携サービスのシステムや、そのシステムに参加する各サーバ 2 5 のセキュリティーポリシーによる。セキュリティーポリシーによっては、イニシエータ署名としてそれら両方の電子署名を施すことも考えられる。

【 0 0 3 8 】

これに対し、包括指示書 6 0 のデータから各サーバ 2 5 宛の個別指示書 6 2 や包括指示書 6 0 a、6 0 b を作成した場合、それら新たに作成した指示書にとっては、元の指示書 6 0 に付されていたイニシエータ署名は無効となってしまう。このため、フロー制御装置 2 0 や別のサーバ 2 5 を介して指示書を受け取るサーバ 2 5 は、その指示書がイニシエータからの正しいものなのかを検証することができない。

【 0 0 3 9 】

以上のようなイニシエータ署名についての問題を解決するための本実施形態の仕組みを、以下に説明する。

【 0 0 4 0 】

この仕組みの基本的な考え方は、指示入力装置 1 0 が包括指示書 6 0 を作成する際、その包括指示書 6 0 に組み込む各サーバ 2 5 宛の個別指示書 6 2 に対し、それぞれ個別にイニシエータ署名を施すというものである。

【 0 0 4 1 】

この考え方に従った、図 3 の指示送信形態に好適な包括指示書の構成を、図 5 を参照して説明する。

【 0 0 4 2 】

図 5 に示す包括指示書 7 0 は、図 3、4 に示した包括指示書 6 0 に対応するも

のであり、3つのサーバ25-1, 25-2, 25-3への各署名済み個別指示書72-1, 72-2, 72-3を含んでいる。各署名済み個別指示書72-1, 72-2, 72-3は、平文の個別指示書62-1, 62-2, 62-3に対してそれぞれイニシエータ署名74-1, 74-2, 74-3を付加したものである。

【0043】

このような包括指示書70を用いた場合、フロー制御装置20は、包括指示書70から各署名済み個別指示書72-1, 72-2, 72-3を取り出して対応するサーバ25-1, 25-2, 25-3に送信することになる。各サーバ25は、受信した署名済み個別指示書72に含まれるイニシエータ署名74を検証することで、その個別指示書72の真正性等を検査できる。

【0044】

また、図5の包括指示書70には、これら署名済み個別指示書72-1, 72-2, 72-3の全体に対するイニシエータ署名76が含まれている。この全体に対するイニシエータ署名76は、指示入力装置10からこの包括指示書70を受信したフロー制御装置20が、その指示書70の真正性等を検証するのに用いられる。また、この全体に対するイニシエータ署名76は、個々の署名済み個別指示書72-1, 72-2, 72-3の流用を防ぐためにも効果がある。

【0045】

すなわち、本実施形態の方式では、包括指示書70に含まれている個別指示書72にイニシエータ署名74が付されているので、例えばインターネット上の第三者が、様々な包括指示書70を集めてそれらから署名済み個別指示書72を取り出し、再組み立てして別の包括指示書を作成し不正利用するおそれがある。これに対し、図5の例のように、包括指示書70中に含まれるすべての署名済み個別指示書72を併せたものに対してイニシエータ署名76を付加すれば、そのような不正な再組み立てによって作成された包括指示書は、フロー制御装置20での署名検証で検出できるので、不正利用を防止できる。

【0046】

なお、包括指示書70から取り出した署名済み個別指示書72をサーバ25に

直接送るという方法での不正利用も考えられる。しかしながら、これに対しては、フロー制御装置 2 0 が署名済み個別指示書 7 2 に対して当該装置 2 0 自身の秘密鍵で電子署名を付加し、サーバ 2 5 側でその装置 2 0 の電子署名を検証することで、そのような不正を検出できる。

【 0 0 4 7 】

次に、この包括指示書 7 0 の具体例を説明する。

【 0 0 4 8 】

ここでは、説明のために、指示入力装置 1 0 で読み取った複数のページを有する文書ファイルから第 1 ページのデータを取り出し、所定の宛先に電子メールで送信するという連携サービスを表す包括指示書を考える。包括指示書が使用されるシステムとしては、図 3 に示したフロー制御装置介在型のシステムを考える。このシステムにおいて、サーバ 2 5 - 1 がページばらし（文書ファイルをページ単位のファイルに分割し、要求されたページのファイルを返す処理）のサービスを提供し、サーバ 2 5 - 2 が電子メール送信サービスを提供するものとする。またサーバ 2 5 - 1 は“pagedivider.foo.jp”というホスト名を有し、サーバ 2 5 - 2 は“mailsender.foo.jp”というホスト名を有するものとする。この指示書 7 0 に示される連携サービスでは、指示入力装置 1 0 にて紙原稿の読み取りが行われ、サーバ 2 5 - 1 にて読み取り結果の文書ファイルから第 1 ページが抽出され、サーバ 2 5 - 2 にてその第 1 ページのファイルを含んだ電子メールが作成され、所定宛先に送られることになる。

【 0 0 4 9 】

このような連携サービスを記述した平文の包括指示書 6 0 は、図 6 に示すような記述となる。

【 0 0 5 0 】

図 6 の包括指示書 6 0 は、XML (eXtended Markup Language) で記述されている。この包括指示書 6 0 は、この指示書 6 0 で使用している XML のバージョンや文字コードを示す文書要素 6 0 5 と、この指示書 6 0 が表す連携サービスを示す文書要素 6 1 0 とを含んでいる。連携サービスを示す要素 6 1 0 のタグには、この連携サービスの名称 (name=“report delivery”) が示されている。そして、

この要素 6 1 0 には、それら連携サービスを担う各サーバ 2 5 - 1, 2 5 - 2 に対する個別指示書 6 2 0 a, 6 2 0 b とが記述されている。

【 0 0 5 1 】

個別指示書 6 2 0 a の記述 6 2 2 a には、連携サービス中での当該処理の順番 (order="1")、及び当該処理を実行するサーバ 2 5 - 1 のホスト名 (url="page divider.foo.jp") が示されている。また、記述 6 2 4 a の 1 行目には、そのサーバ 2 5 - 1 が提供する各種の処理のうち、今回利用する処理の名称 (jobname="ExtractFrontPage") が示される。例えば、サーバ 2 5 - 1 は、文書ファイルから先頭ページを取り出してその先頭ページのファイルを作成する処理の他に、文書ファイルをページ単位にばらして各ページごとのファイルを作成する処理などの様々な処理ができる。記述 6 2 4 a の 1 行目は、それら様々な処理のうち、文書ファイルの先頭ページのファイルを作成する処理を示すものである。また記述 6 2 4 a の 2 行目及び 3 行目にはその処理のパラメータが示されている。2 行目のパラメータは、その処理に対する入力ファイルのファイル名 ("ExtractFrontPage") を示し、3 行目のパラメータはその処理の出力ファイルのファイル名 ("ExtractedPage") である。指示入力装置 1 0 が、読み取った原稿を示す文書ファイルに対し、"ExtractFrontPage" というファイル名を付し、この指示書 6 0 に添付して送信すれば、サーバ 2 5 - 1 でそのファイルが処理対象であると認識できる。

【 0 0 5 2 】

また、個別指示書 6 2 0 a は、この指示書が示す処理の後に処理を行うサーバ 2 5 - 2 を示す記述 6 2 6 a を含んでいる。この記述 6 2 6 a には、次のサーバ 2 5 - 2 のホスト名 (url="pagedivider.foo.jp") が示されている。

【 0 0 5 3 】

サーバ 2 5 - 2 に対する個別指示書 6 2 0 b は、上記個別指示書 6 2 0 a と同様、処理の順序及びサーバ 2 5 - 2 のホスト名を示す記述 6 2 2 b と、そのサーバ 2 5 - 2 が行うべき処理の名称及びその処理のパラメータを示す記述 6 2 4 b を含んでいる。サーバ 2 5 - 2 が行う処理は、電子メールの送信処理なので、パラメータとしては電子メールの宛先アドレス (記述 6 2 4 b の 2 行目) と、その

電子メールに添付されるファイルの名称（記述 6 2 4 b の 3 行目）とを含んでいる。なお、添付されるファイルの名称は、サーバ 2 5 - 1 の処理の出力ファイル名と同じものとなっている。

【 0 0 5 4 】

なお、サーバ 2 5 - 2 は、この包括指示書 6 0 が示す連携サービスの中の最後の処理なので、次のサーバを示す記述は含まれていない。

【 0 0 5 5 】

このような平文の包括指示書 6 0 に対するに、図 5 に示した考え方に従ってイニシエータ署名を施した包括指示書 7 0 の記述は図 7 に示すようなものとなる。なお、図 7 の例は、説明のために簡略化を行っている。

【 0 0 5 6 】

図 7 の記述例では、包括指示書 7 0 は、サーバ 2 5 - 1 に対する署名済み個別指示書 7 2 0 と、サーバ 2 5 - 2 に対する署名済み個別指示書 7 3 0 を含んでいる。

【 0 0 5 7 】

サーバ 2 5 - 1 宛の署名済み個別指示書 7 2 0 は、<Signature> タグ 7 2 2 で示されるエンベローピング署名形式の署名要素として記述される。この署名要素の中には、まず電子署名に用いたアルゴリズムなどの情報を示す署名情報要素 7 2 6 が記述される。この例では署名アルゴリズムとして S H A - 1 (RFC3174) が用いられている。その次に<object>, </object> タグで挟まれた署名対象要素 S が記述される。この署名対象要素 S は、平文の包括指示書 6 0 の個別指示書 6 2 0 a（図 6 参照）と同じ記述内容である。また、要素 7 2 4 は、署名対象要素 S に対し、イニシエータの秘密鍵と指定された署名アルゴリズムから求めた署名値を示す署名値要素である。図 7 では省略しているが、署名済み個別指示書 7 2 0 内には、署名値要素 7 2 4 を計算するのに用いた秘密鍵に対応する公開鍵を示す鍵情報要素（<KeyInfo> タグで示される）が含まれる。後段のサーバがその署名を検証する場合は、その鍵情報要素の情報に基づき、署名鍵に対応する公開鍵を取得し、この公開鍵を用いて署名検証を行うことになる。

【 0 0 5 8 】

同様に、サーバ 2 5 - 2 宛の署名済み個別指示書 7 3 0 は、タグ 7 3 2 で示される署名要素内に、署名情報要素 7 3 6、署名対象要素 T（個別指示書 6 2 0 b）、その要素 T に対するイニシエータ署名値を示す署名値要素 7 3 4 及び鍵情報要素が含まれる。

【 0 0 5 9 】

そして、包括指示書 7 0 全体は、これら 2 つの署名済み個別指示書 7 2 0 及び 7 3 0 をマージした署名対象要素 U に対し、イニシエータ署名を施したものとなる。すなわち、包括指示書 7 0 は、<Signature> タグ 7 1 2 で示される署名要素の中に、署名情報要素 7 1 6、署名対象要素 U、及びその要素 U に対するイニシエータ署名値を示す署名値要素 7 1 4 及び鍵情報要素を含んだものとなる。

【 0 0 6 0 】

次に、図 4 に示した第 2 の指示送信形態に好適な包括指示書の構成を、図 8 を参照して説明する。

【 0 0 6 1 】

図 8 の包括指示書 8 0 では、まず各個別指示書 6 2 - 1、6 2 - 2、6 2 - 3 が、それぞれイニシエータ署名 8 4 - 1、8 4 - 2、8 4 - 1 を付されることで、署名付き個別指示書 8 2 - 1、8 2 - 2、8 2 - 3 となっている。更に、連携サービス中での処理順序が最後の署名付き個別指示書 8 2 - 3 と 1 つ前の署名付き個別指示書 8 2 - 2 とをマージ（併合）した記述に対してイニシエータ署名 8 7 を付すことで、ブロック 8 5 が形成されている。そして、このブロック 8 5 にもう 1 つ前（そしてこの例では指示書中の先頭）の署名付き個別指示書 8 2 - 1 をマージした記述に対し、イニシエータ署名 8 8 が付されている。この最外郭のイニシエータ署名 8 8 は、図 5 の構成における包括指示書全体に対するイニシエータ署名 7 6 に対応する。

【 0 0 6 2 】

このようにイニシエータ署名が入れ子的に施された包括指示書 8 0 は、各署名付き個別指示書 8 2 - 1、8 2 - 2、8 2 - 3 に対し、処理順序の逆順に、「署名結果に対し 1 つ前の署名付き指示書をマージしてイニシエータ署名を施す」という処理を再帰的に適用することで作成することができる。すなわち、この署名

処理では、電子署名付与の対象とする処理記述（すなわち個別指示書）より後に、処理を実行すべき処理記述を含めて署名している。

【0063】

指示入力装置 10 でこのような包括指示書 80 を作成し、最初のサーバ 25-1 に送信すると、そのサーバ 25-1 は、まず包括指示書 80 全体に対するイニシエータ署名 88 を検証する。この検証が成功した場合、サーバ 25-1 は、自分宛の署名付き個別指示書 82-1 を探し、その指示書 82-1 のイニシエータ署名 84-1 を検証する。この検証が成功すると、サーバ 25-1 は、その指示書 82-1 の記述に従って処理を実行すると共に、次のサーバ 25-2 宛の包括指示書 80a を作成する。この包括指示書 80a は、基となる包括指示書 80 から、サーバ 25-1 宛の署名付き個別指示書 82-1 と最外郭のイニシエータ署名 88 を取り除いて残るブロック 85 に対し、XML フォーマットの包括指示書として必要なタグ等を付加することにより作成される。すなわち、包括指示書 80a では、ブロック 85 のイニシエータ署名 87 が、包括指示書 80a 全体に対するイニシエータ署名となる。

【0064】

次に、包括指示書 80a を受け取ったサーバ 25-2 も、同様に指示書 80a 全体のイニシエータ署名、及び自分宛の署名付き個別指示書 82-2 のイニシエータ署名を検証し、それら検証が共に成功すれば、その指示書 82-2 の処理を実行し、その次のサーバ 25-3 宛の包括指示書 80b を作成する。この包括指示書 80b も、上記と同様、基となる包括指示書 80a から署名付き個別指示書 82-2 と最外郭のイニシエータ署名 87 を取り除き、この結果残る署名付き個別指示書 82-3 に対し、包括指示書として必要なタグ等を付加することにより作成される。

【0065】

サーバ 25-3 は、その包括指示書 80b を受け取ると、その中に含まれる自分宛の署名付き個別指示書 82-3 のイニシエータ署名を検証し、検証が成功すると、その指示書に示される処理を実行する。これにより、包括指示書 80 に対応する連携サービスが完了する。

【0066】

このように、図8に示す入れ子構造の包括指示書80では、連携サービスのフロー中のどのサーバ間をとっても、前のサーバ25から次のサーバ25に受け渡す指示書の基になるデータブロック（すなわち該次のサーバ以降の各サーバへの指示書群）全体に対し、イニシエータ署名が必ず付されていることになる。したがって、各サーバ25は、前のサーバ25から受け取った包括指示書から、自分宛の個別指示書を取り除くことで、次のサーバ25に対し、全体に対するイニシエータ署名が付いた包括指示書を作成できる。

【0067】

したがって、図8の包括指示書80の構造でも、サーバ25から次のサーバ25に送られる包括指示書は、常にその包括指示書全体に対してイニシエータ署名が付されているので、第三者が個々の署名付き個別指示書82を再組み立てして包括指示書を作成するといった不正行為を防止することができる。

【0068】

次の、図8の包括指示書80の具体例を、図9を参照して説明する。

【0069】

図9の具体例は、指示入力装置10で読み取った複数のページを有する文書ファイルから第1ページのデータを取り出し（サービスA）、それを所定のファイルフォーマットに変換（サービスB）してから、所定の宛先に電子メールで送信する（サービスC）という、3つのサービスからなる連携サービスを表す。これら3つのサービスのうち、サービスA及びCは、図6及びの例におけるページばらし及び電子メール送信と同じ処理内容なので一部の記述を省略している。

【0070】

図9の記述例では、各署名付き個別指示書820、830、及び840に対し、それぞれ署名対象要素V、W、Xに対するイニシエータ署名824、834、及び844が付されている。そして、署名付き子個別指示書830と840とを併合した署名対象要素Yに対し、イニシエータ署名854が付されている。そして、署名対象要素Yとイニシエータ署名854からなる署名要素850にその前の署名付き個別指示書820を併合した署名対象要素Zに対し、イニシエータ署

名 814 が付されることで、全体としての包括指示書 80 が構成されている。

【0071】

以上、図 3 及び図 4 の各指示送信形態に対応する包括指示書 70 及び 80 のデータ構造を説明した。図 7 及び図 9 に示した包括指示書 70 及び 80 の記述は、XML-signature (RFC3275) のエンベローピング(enveloping)署名形式を用いた場合の例である。しかしながら、当業者ならば明らかなように、本実施形態の方式は、署名形式に依存するものではない。また更には、本実施形態の方式は、XML などといった指示書のデータフォーマットに依存するものでもない。

【0072】

以上、本実施形態の署名処理について説明した。本実施形態は、指示書に対する電子署名に関するものであるため、暗号化などの側面については触れずに説明してきた。しかしながら、当業者ならば明らかなように、上述の本実施形態の署名処理を、必要に応じて暗号化処理と組み合わせることは可能である。例えば、各個別指示書 620 a や 620 b の処理内容の記述 624 a や 624 b (図 6 参照) に対し、それぞれその個別指示書の宛先であるサーバの公開鍵で暗号化処理を施し、その暗号化結果に対してイニシエータ署名を施すことで、署名付き個別指示書を作成することもできる。また、逆に署名付き個別指示書に対して宛先サーバの公開鍵で暗号化を施すこともできる。

【0073】

以上、本実施形態のシステムの構成及び動作について説明した。以上の実施形態では、第 1 段階として、連携サービスのために連携動作する各サーバへの個別指示書に対し、それぞれ個別にイニシエータ署名を施した。このときの署名処理の単位となる「サーバ」は、あるサービス処理を記述したアプリケーションプログラムをコンピュータで実行させることにより実現される仮想機械であってもよいし、そのようなアプリケーションプログラムを 1 乃至複数備えたハードウェア装置であってもよい。前者の場合は、アプリケーションごとの処理の記述が 1 つの個別指示書となるのに対し、後者の場合は 1 つのハードウェア装置に含まれる複数のアプリケーションの処理の記述を順に並べたものが 1 つの個別指示書となる。

【0074】

次にこのシステムを構成する指示入力装置10、フロー制御装置20及び各サーバ25の内部構成の一例を、図10を参照して説明する。

【0075】

まず、指示入力装置10について説明する。指示入力装置10のUI（ユーザ・インタフェース）102は、指示入力装置10の状態や操作メニュー等を表示し、これに対するユーザの選択やパラメータ入力を受け取るユーザ・インタフェース機構であり、例えば液晶タッチパネルやテンキーボタン、各種の指示ボタンを備える。処理モジュール104は、当該指示入力装置10自体がユーザに提供するサービス処理を実行する処理モジュールである。指示入力装置10が複合機である場合、処理モジュール104には、スキャン機能、プリント機能、コピー機能、ファクシミリ送受信機能等を実現する機能モジュールが含まれる。この場合、これら処理モジュール104は、スキャンエンジンやプリントエンジン、ファクシミリ装置等のハードウェアと、それら各ハードウェアを制御するソフトウェアの組合せにより構成される。通信制御部106は、この指示入力装置10とLAN等のネットワーク35上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【0076】

暗号・復号処理部108は、指示入力装置10からネットワーク35に送信するデータに対して暗号化を行ったり、送信されてきた暗号化されたデータを復号したりする機能モジュールである。ここでは、暗号・復号処理部108は、暗号方式として公開鍵暗号方式をサポートしているものとする。ただし、これは一例であり、暗号・復号処理部108は、共通鍵方式など他の暗号方式を基礎とするものであってもよい。

【0077】

暗号・復号処理部108で用いる暗号化処理の一例としては、乱数等で発生したセッション鍵（共通鍵）を用いて対象となる文書データを暗号化し、このセッション鍵を送信先の公開鍵で暗号化し、これら両暗号化データを送信先へに送信するという処理を挙げることができる。受信側では、受け取ったデータを自らの

秘密鍵で復号することでセッション鍵を得、暗号化された文書データをそのセッション鍵により復号する。本明細書中で「公開鍵で暗号化する」といった場合、文字通り公開鍵を用いて対象データを暗号化する場合のみならず、このようなセッション鍵を利用する暗号化処理の場合もあるものとする。

【 0 0 7 8 】

また、暗号・復号処理部 1 0 8 は、送信するデータに対して電子署名を施したり、受信したデータに付された電子署名を検証したりする機能を備える。電子署名は、例えば署名対象の文書データから S H A - 1 や M D 5 (RFC1321)等の所定ダイジェスト方式に従って求めたメッセージダイジェストを、署名者の秘密鍵で暗号化することにより得られる。この電子署名の検証は、該署名データを署名者の公開鍵で復号し、その復号化結果が、署名対象の文書データから所定ダイジェスト方式に従って求めたメッセージダイジェストと一致するか否かを判定することにより行われる。一致すれば、該文書データが署名者からの真正なデータであることが証明されると共に、該文書データに対して改竄が加えられていないことが証明される。

【 0 0 7 9 】

上述した本実施形態の電子署名処理は、この暗号・復号処理部 1 0 8 にて実行される。

【 0 0 8 0 】

ここで暗号・復号処理部 1 0 8 は、少なくともフロー制御装置 2 0 の公開鍵を保管している。また暗号・復号処理部 1 0 8 に、各サーバやユーザの公開鍵をネットワーク上の所定の認証局等から必要に応じて取得する機能を設けることも好適である。また暗号・復号処理部 1 0 8 は、該指示入力装置 1 0 自身の秘密鍵を備え、該指示入力装置 1 0 の電子署名を行うことができる。

【 0 0 8 1 】

トークン I / F (インタフェース) 1 1 0 は、ユーザが保持するハードウェアトークンを受け入れ、このトークンと通信することで該ユーザの秘密鍵による電子署名を取得する機構である。ここでハードウェアトークンは、ユーザが携帯する小型の認証デバイスである。公開鍵暗号方式を利用する場合、ハードウェアト

ークンは、例えば、ユーザの秘密鍵データを記憶する記憶チップと、署名対象のデータに対してユーザの秘密鍵を用いて暗号化を施すことにより署名データを生成する演算回路と、署名対象のデータの入力及び署名データの出力のためのインタフェース機構とを備えるものとなる。ハードウェアトークンは、例えば接触読み取り式又は非接触読み取り式の IC カード、USB (Universal Serial Bus) 等の各種有線インタフェース規格に対応したデバイス、或いはBluetooth等の各種無線インタフェース規格に対応したデバイスなどとして構成される。

【0082】

包括指示書に対するイニシエータ署名として、サービスを依頼するユーザの電子署名が要求される場合は、このトークン I/F 110 を介してユーザのハードウェアトークンからイニシエータ署名の付与を受ける。

【0083】

この構成では、通信制御部 106 は、送信すべきデータに対してユーザの電子署名を行う必要がある場合、例えば MD5 などの方式に従ってそのデータのメッセージダイジェストを作成し、これをトークン I/F 110 に装着されたハードウェアトークンに入力する。ハードウェアトークンは、入力されたメッセージダイジェストを、保持しているユーザの秘密鍵で暗号化し、その暗号化処理結果（すなわちユーザの署名）を通信制御部 106 に返す。このユーザ署名を通信制御部 106 が文書データに付加することにより、文書データに対するユーザの電子署名が為される。

【0084】

以上ではユーザのハードウェアトークンを利用してユーザの電子署名を行う方法を説明したが、別の方式として、指示入力装置 10 内にユーザの秘密鍵を予め保管しておき、この秘密鍵を用いて上述と同様の処理により該ユーザの電子署名を行う方式も可能である。この方式では、ユーザの秘密鍵保護のため、ユーザにパスワードやバイオメトリクス等の認証情報の入力を求め、これによりユーザ認証が成功した場合に限り、そのユーザの電子署名を認めるという制御を必須とする。ハードウェアトークンを用いる構成の場合、ユーザ署名が必要な連携サービスを行うと、最悪の場合その連携サービスが完了するまで指示入力装置 10 にト

ークンをセットしたまま待っている必要があるが、指示入力装置 10 に秘密鍵を保管する構成ではそのような待機は必要ない。逆に、ハードウェアトークンを用いる構成は、ユーザは、どの複合機その他の装置からでも、ユーザ署名が必要な連携サービスを実行できるという利点がある。

【0085】

以上、指示入力装置 10 の構成の一例を説明した。このような指示入力装置 10 は、コンピュータや上述の複合機など、プログラムを実行して情報処理を実行することができる装置に、上述の各種の機能を記述したプログラムを実行させることによって実現できる。

【0086】

次に、フロー制御装置 20 の構成について説明する。これは、上述の第 1 の指示送信形態（図 3）に対応するものであり、第 2 の指示送信形態（図 4）の場合は、このフロー制御装置 20 は必要ない。

【0087】

フロー制御装置 20 において、ユーザ管理部 202 は、該サーバ 20 がサービス対象とするユーザについての各種情報を管理している。ユーザ管理部 202 が管理する情報には、例えばユーザの認証に用いる認証情報（パスワードやバイオメトリクス情報など）や、ユーザが登録している UI 画面情報などがある。すなわち、本実施形態のシステムでは、ネットワーク 35 上の各種サーバ装置が提供するサービスをユーザが組み合わせることで、ユーザ固有の連携サービスを定義可能としており、これらユーザ固有の連携サービスを指示できる該ユーザ固有の UI 画面をフロー制御装置 20 から提供する。

【0088】

この場合、ユーザ（個人の場合もあれば、複数人からなるグループの場合もある）が指示入力装置 10 に認証情報を入力して認証が成功すると、指示入力装置 10 がフロー制御装置 20 に当該ユーザの UI 画面を要求する。この要求に応じ、フロー制御装置 20 は、そのユーザが登録した連携サービスのメニュー等を含んだ UI 画面を、そのユーザの公開鍵で暗号化した上で指示入力装置 10 に送信する。ユーザが、指示入力装置 10 のディスプレイに表示されたその UI 画面上

で、使用したい連携サービスを選択すると、その選択内容がフロー制御装置 2 0 の公開鍵で暗号化された上で、指示入力装置 1 0 からフロー制御装置 2 0 に送られる。この選択結果を受けとったフロー制御装置 2 0 は、ユーザが選択した連携サービスを示す包括指示書のひな形データを、ユーザの公開鍵で暗号化した上で、指示入力装置 1 0 に送信する。指示入力装置 1 0 は、この包括指示書のひな形の中に、ユーザが入力しなければならないパラメータが含まれる場合、そのパラメータの入力画面を U I 1 0 2 に表示し、ユーザの入力を求める。このようにしてパラメータ群が入力されると、包括指示書が完成する。これが上述のフロー指示書 5 0 に対応する。指示入力装置 1 0 は、完成したフロー指示書をフロー制御装置 2 0 の公開鍵で暗号化した上で、フロー制御装置 2 0 に送信する。

【0 0 8 9】

ユーザによるフロー制御装置 2 0 への連携サービスの登録処理や、フロー制御装置 2 0 から指示入力装置 1 0 に提供する各ユーザ固有の U I 画面の情報については、本実施形態の要旨とは直接関係しないので説明を省略するが、これらについては本出願人による特願 2 0 0 2 - 2 7 5 2 2 9 号、特願 2 0 0 2 - 2 7 5 2 3 0 号、特願 2 0 0 2 - 2 7 5 2 3 1 号に開示されているので、必要があれば参照されたい。

【0 0 9 0】

なお、この例は、U I 画面の情報や連携サービスの包括指示書のひな形はフロー制御装置 2 0 が保管し、随時指示入力装置 1 0 に提供する構成であったが、それら U I 画面や包括指示書のひな形を指示入力装置 1 0 に保管しておくこともできる。

【0 0 9 1】

フロー制御部 2 0 4 は、ユーザが要求した連携サービスを実現するために、連携サービスにおいて規定されるフローに従って各サーバ 2 5 や指示入力装置 1 0 に対して必要な処理の実行依頼を行う機能モジュールである。すなわち、連携サービスは、各サーバ 2 5 が提供する 1 以上の処理（以下では単位ジョブとも呼ぶ）からなるフローとして定義され、フロー制御装置 2 0 は、このフロー定義に示される単位ジョブを順に対応するサーバに依頼していく。ここで、各サーバの処

理結果は、必要に応じてフロー制御装置 2 0 に返され、次の単位ジョブの処理対象データとしてフロー制御装置 2 0 から対応するサーバへと送信される。フロー制御部 2 0 4 は、このような各サーバ、複合機への処理依頼と、これに対する処理結果の取得などの処理を実行する。

【 0 0 9 2 】

なお、指示入力装置 1 0 が、連携サービスの指示受付機能の他にも処理機能を備え、この処理機能を連携サービスのために提供できる場合もある。この場合、指示入力装置 1 0 は、その処理機能についてはアプリケーションサーバ 2 5 の 1 つととらえることができる。

【 0 0 9 3 】

暗号・復号処理部 2 0 6 は、フロー制御装置 2 0 からネットワーク 3 5 に送信するデータに対して暗号化を行ったり、送信されてきた暗号化データを復号したりする機能モジュールであり、暗号・復号処理部 1 0 8 と同等の暗号化、復号化、電子署名及びその検証の機能を有する。

【 0 0 9 4 】

ここで暗号・復号処理部 2 0 6 は、指示入力装置 1 0 や各サーバ 2 5 などの装置や、各ユーザの公開鍵を保管しているか、又はネットワーク上の認証局等から取得する機能を備える。そして、データを送信する必要が生じた場合は、その送信先の装置やユーザの公開鍵を用いて暗号化を行う。

【 0 0 9 5 】

また、暗号・復号処理部 2 0 6 は、電子署名関連機能の一つとして、指示入力装置 1 0 から送信されてきた包括指示書 7 0 の全体に対するイニシエータ署名 7 6 の検証を行う機能を備える。また、暗号・復号処理部 2 0 6 は、フロー制御装置 2 0 の秘密鍵を備え、送信するデータに対してフロー制御装置 2 0 の電子署名を付することができる。

【 0 0 9 6 】

通信制御部 2 1 2 は、フロー制御装置 2 0 とネットワーク 3 5 上の他の装置との通信のための各種制御処理を行う機能モジュールである。

【 0 0 9 7 】

以上、フロー制御装置 2 0 の構成の一例を説明した。このようなフロー制御装置 2 0 は、上述の各種の機能を記述したプログラムをコンピュータに実行させることによって実現できる。

【 0 0 9 8 】

次にアプリケーションサーバ 2 5 について説明する。アプリケーションサーバ 2 5 は、該サーバが提供するサービスのためのアプリケーションプログラム 2 5 2 と、ネットワーク 3 5 上の他の装置との通信のための制御処理を実行する通信制御部 2 5 4 と、その通信の際の暗号化及び復号の処理を実行する暗号・復号処理部 2 5 6 とを備える。

【 0 0 9 9 】

サーバ 2 5 の暗号・復号処理部 2 5 6 は、フロー制御装置 2 0 又は他のサーバ 2 5 から送られてきた包括指示書に対し、上述のイニシエータ署名検証を行う機能を備える。この署名検証が成功した場合、アプリケーション 2 5 2 による処理が実行される。

【 0 1 0 0 】

また暗号・復号処理部 2 5 6 は、該サーバ 2 5 の処理によって得られたデータを暗号化する機能を備える。そのような処理結果のデータを、フロー制御装置 2 0 又は他のサーバ 2 5 に送る際には、その送り先の公開鍵を用いてそのデータを暗号化する。

【 0 1 0 1 】

また、通信制御部 2 5 4 は、上述の第 1 の指示送信形態（図 3）では、アプリケーション 2 5 2 の処理結果をフロー制御装置 2 0 に送信する処理を行う。また通信制御部 2 5 4 は、第 2 の指示送信形態（図 3）では、次のサーバ 2 5 に対する包括指示書 6 0（及び、必要に応じ、処理結果のデータ）を送信するための上述の処理を実行する。

【 0 1 0 2 】

以上説明した指示入力装置 1 0 及びサーバ 2 5、及びフロー制御装置介在型のシステム構成の場合は更にフロー制御装置 2 0 により、上述の連携サービスのフローが実現されると共に、そのフローにおける各サーバ 2 5 への指示書の秘密を

守る処理が行われる。

【図面の簡単な説明】

【図 1】 連携サービスを提供するシステムの構成の一例を示す図である。

【図 2】 連携サービスを提供するシステムの構成の別の例を示す図である

【図 3】 連携サービスにおける各サーバへの指示書の第 1 の送信形態を説明するための図である。

【図 4】 連携サービスにおける各サーバへの指示書の第 2 の送信形態を説明するための図である。

【図 5】 本実施形態によるイニシエータ署名を施した包括指示書のデータ構造の一例を模式的に示す図である。

【図 6】 平文の包括指示書の例を示す図である。

【図 7】 本実施形態によるイニシエータ署名を施した包括指示書の例を示す図である。

【図 8】 指示入力装置が作成する包括指示書のデータ構造の別の例を模式的に示す図である。

【図 9】 本実施形態によるイニシエータ署名を施した包括指示書の別の例を示す図である。

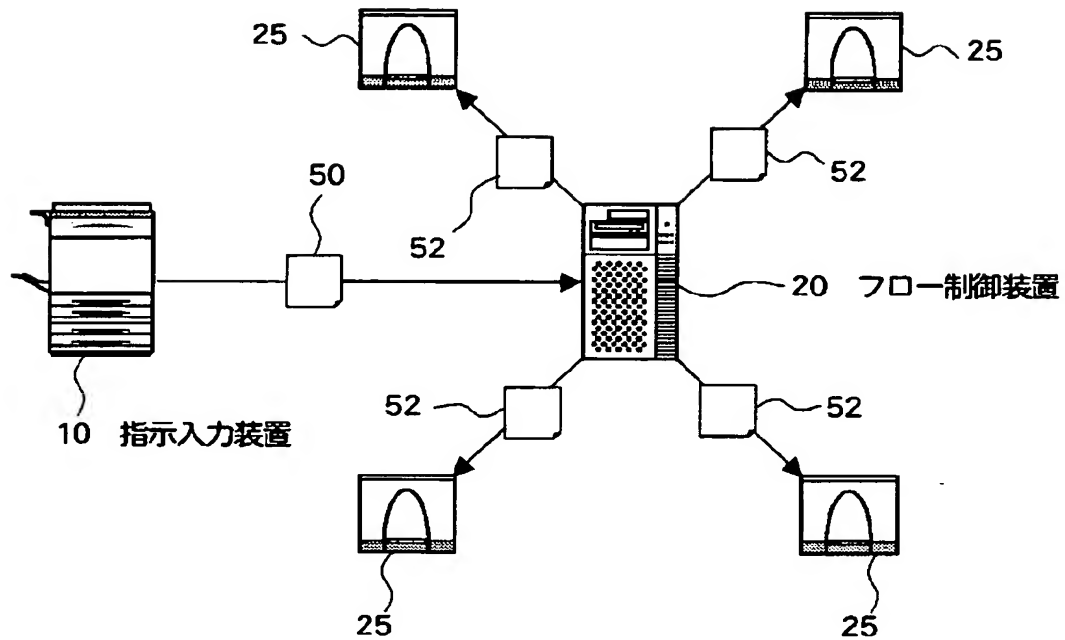
【図 1 0】 連携サービスを提供するシステムを構成する各装置の内部構造の例を示す図である。

【符号の説明】

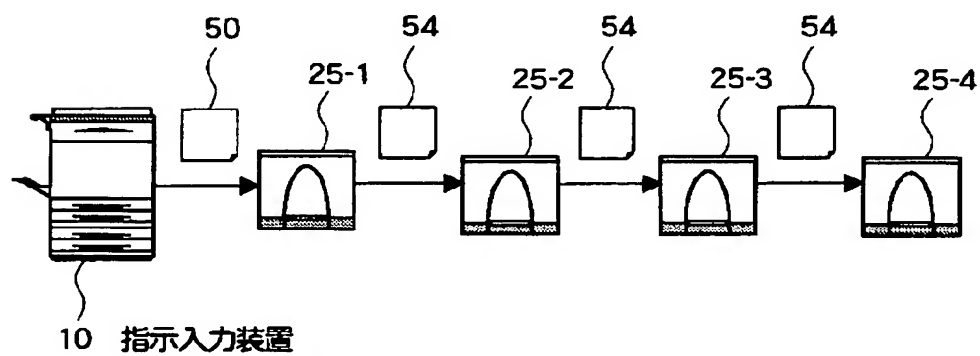
1 0 指示入力装置、2 0 フロー制御装置、2 5 アプリケーションサーバ、5 2, 5 4 指示書、6 0, 7 0 包括指示書、6 2 個別指示書、7 2 - 1, 7 2 - 2, 7 2 - 3 署名済み個別指示書、7 4 - 1, 7 4 - 2, 7 4 - 3, 7 6 イニシエータ署名。

【書類名】 図面

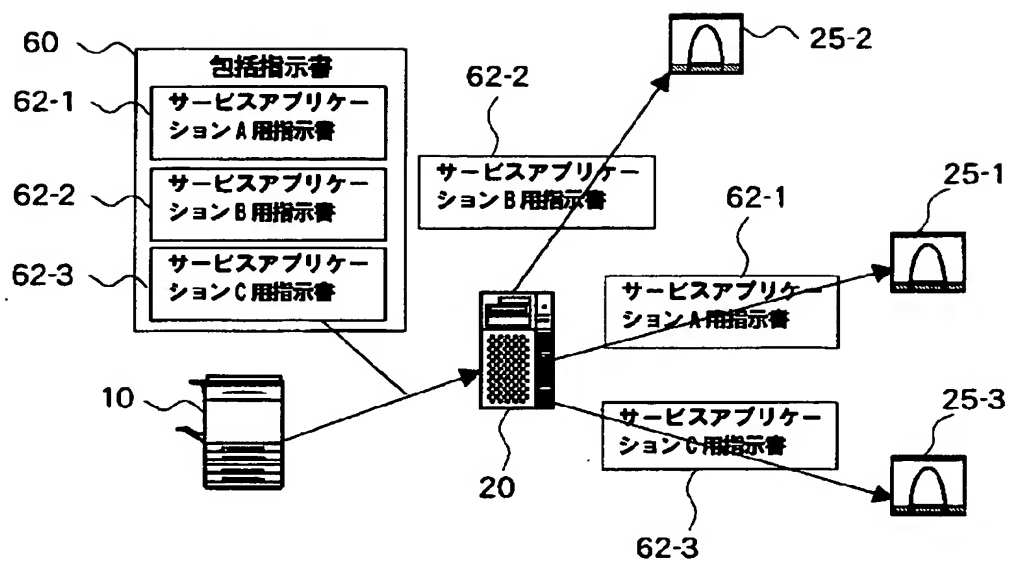
【図 1】



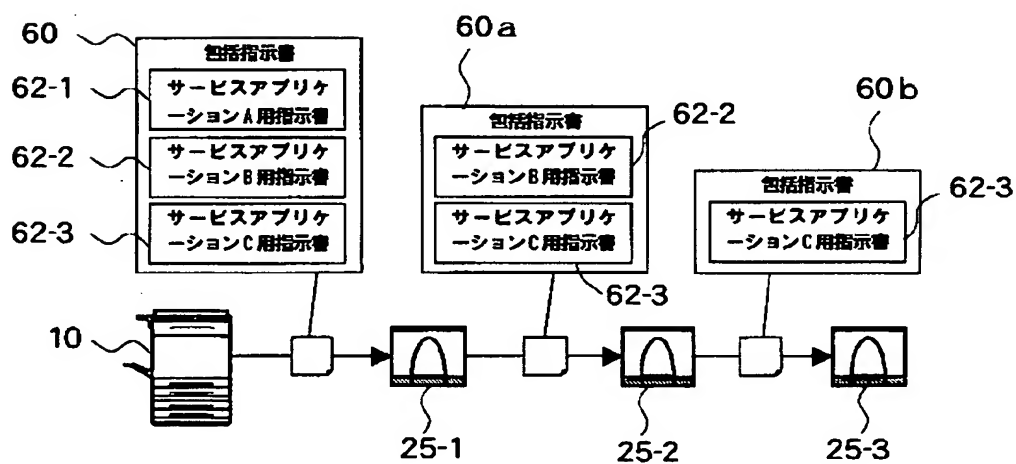
【図 2】



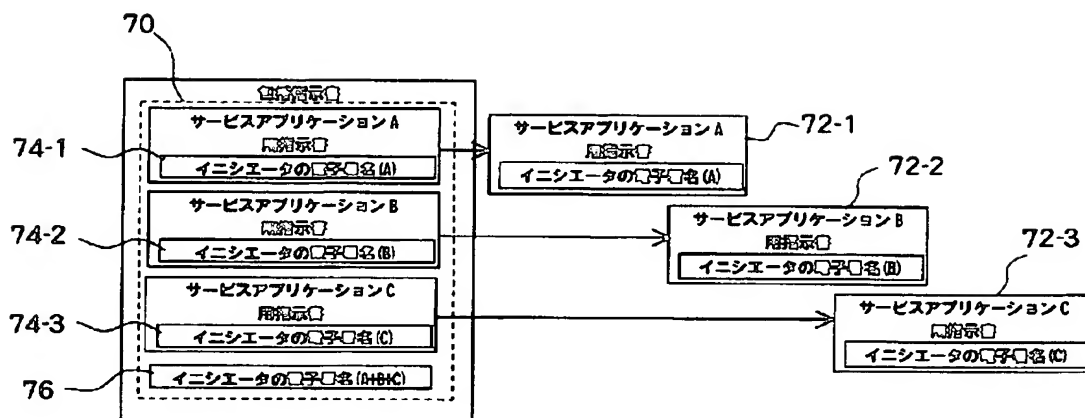
【図 3】



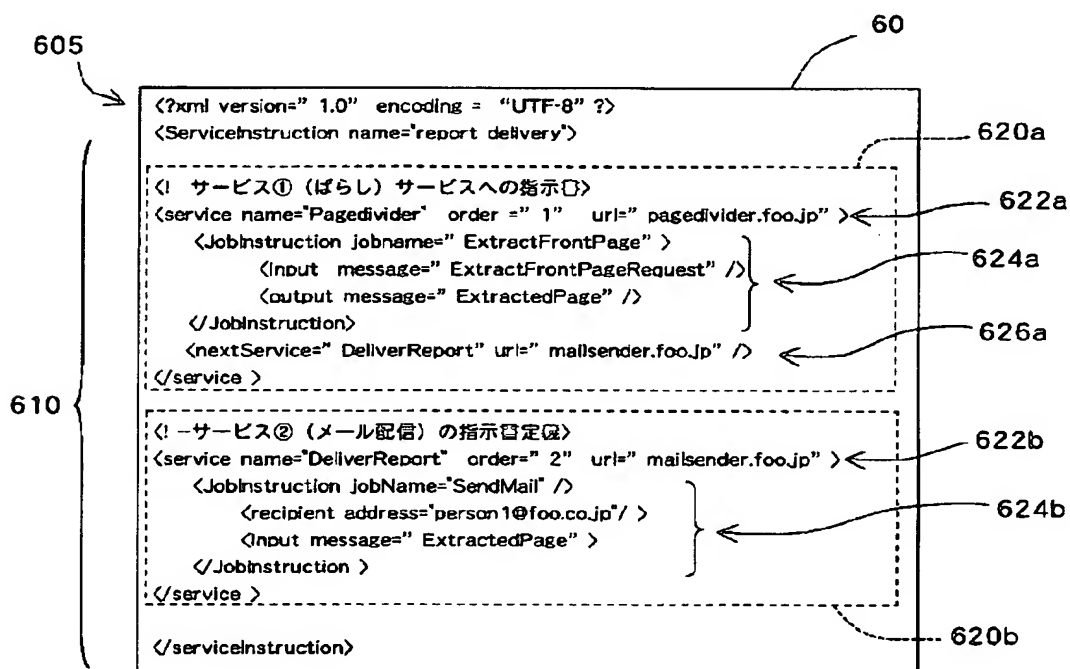
【図 4】



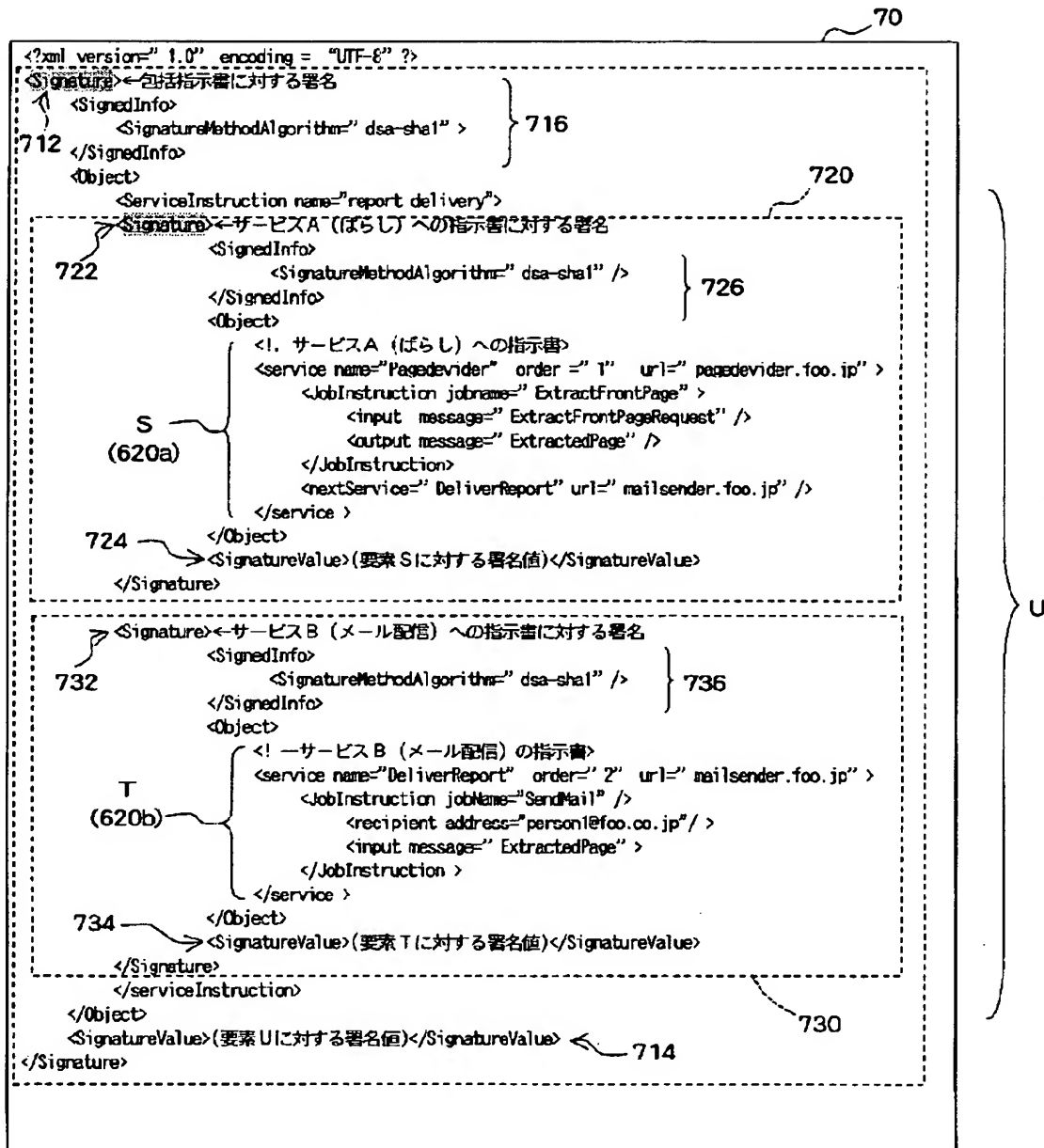
【図 5】



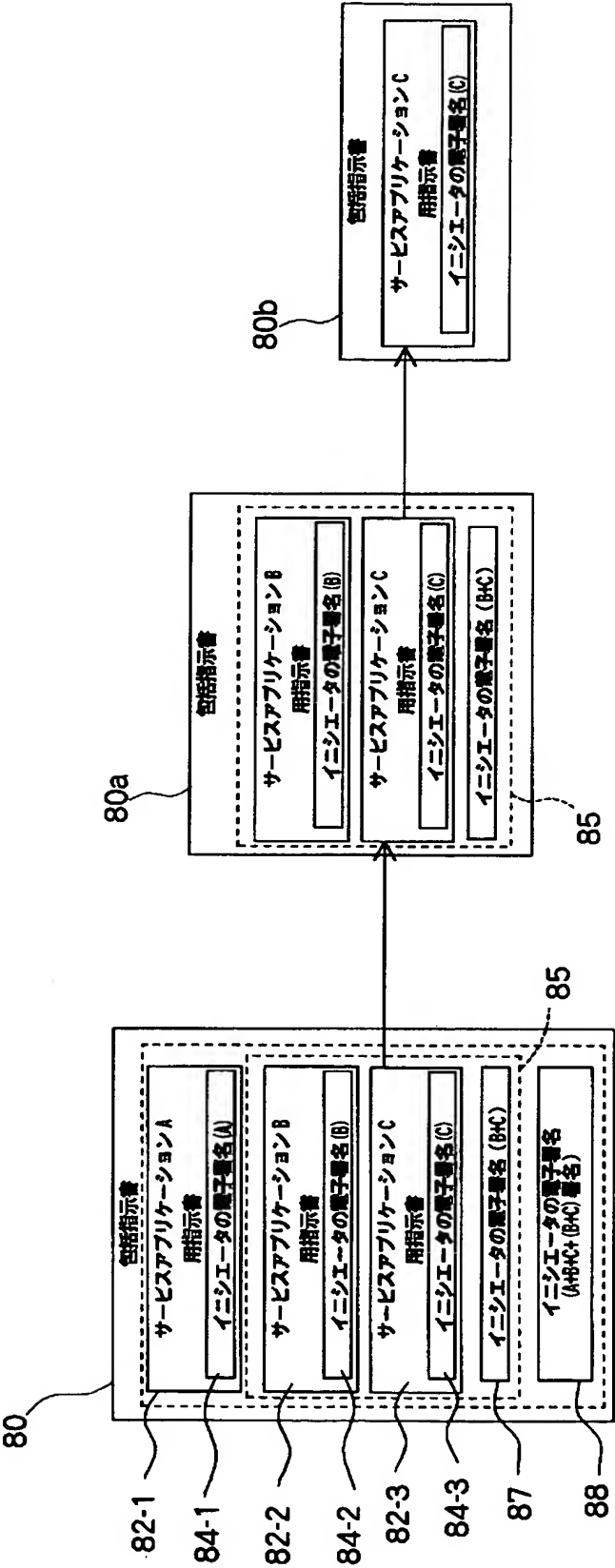
【図 6】



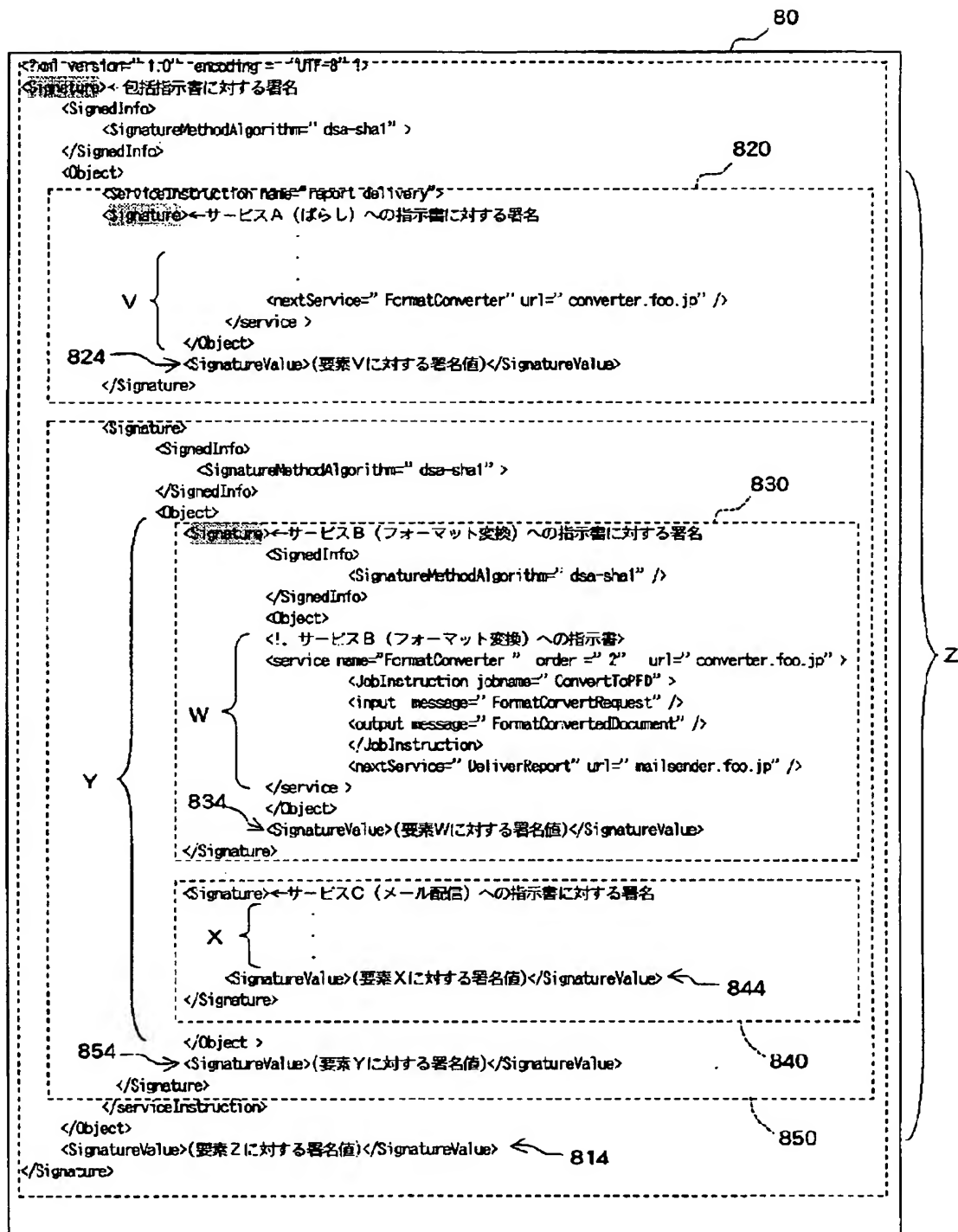
【図 7】



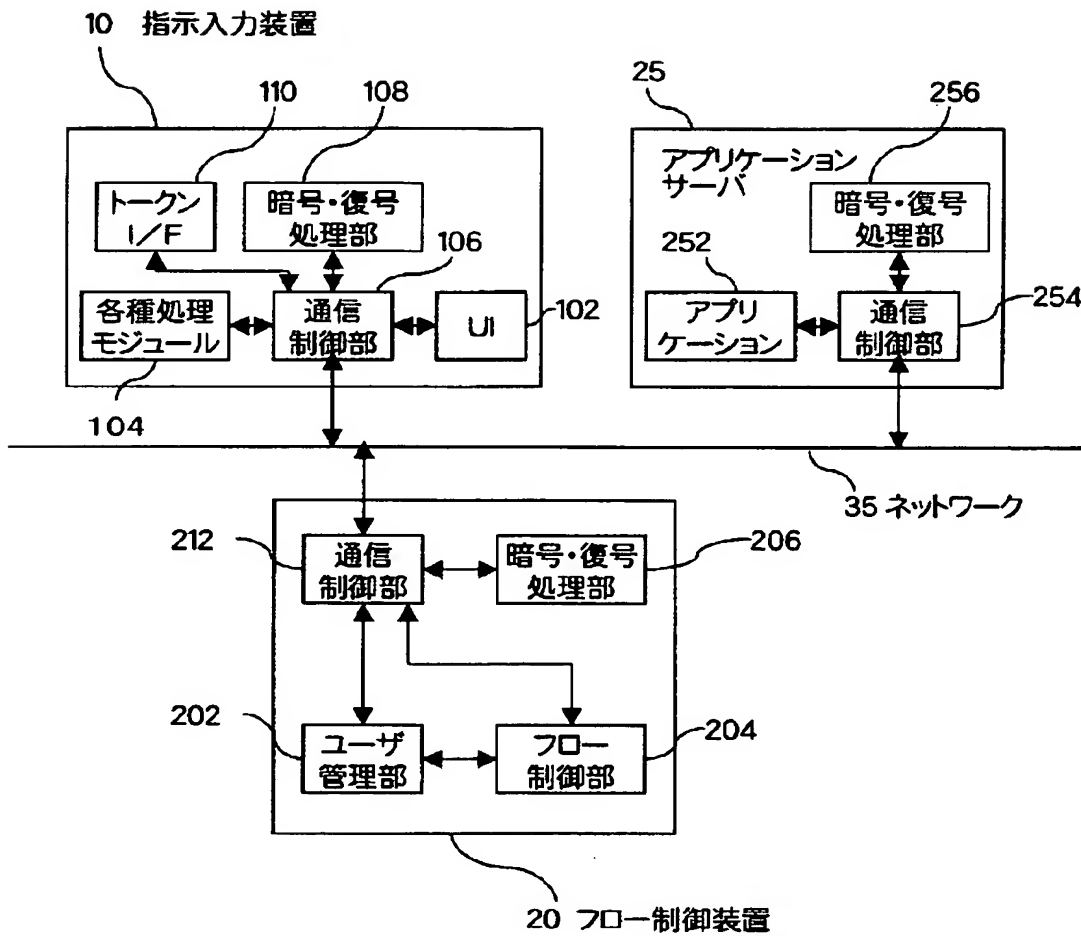
【図 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 各サーバへの指示を示した指示書をそれらサーバ間で受け渡ししながら各サーバが指示書内の各自の指示を実行することで、連携サービスを提供するシステムにおいて、各サーバがサービス指示者の署名を検証できるようにする。

【解決手段】 サービス指示者から指示を受け付けた指示入力装置は、各サーバの処理内容を示した指示書に対して指示者又は当該装置の電子署名（イニシエータ署名 7 4）を付して署名済み個別指示書 7 2 を作成する。そしてサービスに利用するすべてのサーバの署名済み個別指示書 7 2 を併合したのに対してイニシエータ署名 7 6 を付して包括指示書 7 0 を作成する。包括指示書 7 0 は、それらサーバを制御するフロー制御装置に送られる。フロー制御装置はイニシエータ署名 7 6 によりその包括指示書 7 0 の真正性等を検証する。検証が成功すると、フロー制御装置は各サーバに対応する署名済み個別指示書 7 2 を送信する。

【選択図】 図 5

特願 2 0 0 3 - 0 8 2 3 2 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 4 9 6]

1. 変更年月日

1 9 9 6 年 5 月 2 9 日

[変更理由]

住所変更

住 所

東京都港区赤坂二丁目 1 7 番 2 2 号

氏 名

富士ゼロックス株式会社